

We claim

- 1 1. A method comprising:
2 receiving at least one protocol state machine definition for a network protocol, said
3 protocol state machine definition including a plurality of protocol state rules;
4 parsing the at least one protocol state machine definition to form a set of parsed
5 protocol state rules, said parsed protocol state rules including at least one condition and at
6 least one action associated with the condition;
7 storing a set of filters in a filter database;
8 receiving a network flow, said flow including a plurality of packets; and
9 applying the parsed protocol state rules to the plurality of packets in the network flow;
10 wherein the at least one action comprises the instantiation of a filter from the set of
11 filters.
- 1 2. The method of claim 1, wherein the protocol state rules include rules for analyzing a
2 context for the network flow.
- 1 3. The method of claim 2, wherein the context for the network flow includes an
2 application layer context.
- 1 4. The method of claim 1 wherein the filter comprises a dynamic filter that is instantiated
2 for the duration of the network flow.
- 1 5. The method of claim 1, wherein the filter comprises a static filter that is applied during
2 an initiation of the network flow.
- 1 6. The method of claim 1, wherein the at least one action comprises saving the result of
2 the at least one action for use in a later executed rule in the set of parsed protocol state rules.

- 1 7. The method of claim 1, wherein the at least one action comprises deactivating a rule in
2 the set of parsed protocol state rules.
- 1 8. The method of claim 1, wherein the at least one action comprises activating a rule in
2 the set of parsed protocol state rules.
- 1 9. A system comprising:
2 a parser operable to parse at least one protocol state machine definition for a network
3 protocol to a set of parsed protocol state rules, said protocol state machine definition including
4 a plurality of protocol state rules, said parsed protocol state rules including at least one
5 condition and at least one action associated with the condition;
6 a filter database operable to store a set of filters in a filter database; and
7 a protocol analysis engine operable to receive a network flow, said flow including a
8 plurality of packets; and apply the parsed protocol state rules to the plurality of packets in the
9 network flow;
10 wherein the at least one action comprises the instantiation of a filter from the set of
11 filters.
- 1 10. The system of claim 9, wherein the protocol state rules include rules to analyze a
2 context for the network flow.
- 1 11. The system of claim 10, wherein the context for the network flow includes an
2 application layer context.
- 1 12. The system of claim 9 wherein the filter comprises a dynamic filter that is instantiated
2 for the duration of the network flow.

- 1 13. The system of claim 9, wherein the filter comprises a static filter that is applied during
2 an initiation of the network flow.
- 1 14. The system of claim 9, wherein the at least one action comprises saves the result of the
2 at least one action for use in a later executed rule in the set of parsed protocol state rules.
- 1 15. The system of claim 8, wherein the at least one action deactivates a rule in the set of
2 parsed protocol state rules.
- 1 16. The system of claim 9, wherein the at least one action comprises activates a rule in the
2 set of parsed protocol state rules.
- 1 17. The system of claim 9, wherein the protocol analysis engine is further operable to
2 maintain a state table for the network flow.
- 1 18. A machine readable medium having machine executable instructions for performing a
2 method comprising:
3 receiving at least one protocol state machine definition for a network protocol, said
4 protocol state machine definition including a plurality of protocol state rules;
5 parsing the at least one protocol state machine definition to form a set of parsed
6 protocol state rules, said parsed protocol state rules including at least one condition and at
7 least one action associated with the condition;
8 storing a set of filters in a filter database;
9 receiving a network flow, said flow including a plurality of packets; and
10 applying the parsed protocol state rules to the plurality of packets in the network flow;
11 wherein the at least one action comprises the instantiation of a filter from the set of
12 filters.

- 1 19. The machine readable medium of claim 18, wherein the protocol state rules include
2 rules for analyzing a context for the network flow.
- 1 20. The machine readable medium of claim 19, wherein the context for the network flow
2 includes an application layer context.
- 1 21. The machine readable medium of claim 18 wherein the filter comprises a dynamic
2 filter that is instantiated for the duration of the network flow.
- 1 22. The machine readable medium of claim 18, wherein the filter comprises a static filter
2 that is applied during an initiation of the network flow.
- 1 23. The machine readable medium of claim 18, wherein the at least one action comprises
2 saving the result of the at least one action for use in a later executed rule in the set of parsed
3 protocol state rules.
- 1 24. The machine readable medium of claim 18, wherein the at least one action comprises
2 deactivating a rule in the set of parsed protocol state rules.
- 1 25. The machine readable medium of claim 18, wherein the at least one action comprises
2 activating a rule in the set of parsed protocol state rules.